

This Page Is Inserted by IFW Operations
and is not a part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

**As rescanning documents *will not* correct images,
please do not report the images to the
Image Problem Mailbox.**

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 11-306673

(43)Date of publication of application : 05.11.1999

(51)Int.Cl. G11B 20/10
H04L 12/40
// G09C 1/00

(21)Application number : 10-108118

(71)Applicant : TOSHIBA CORP

(22)Date of filing : 17.04.1998

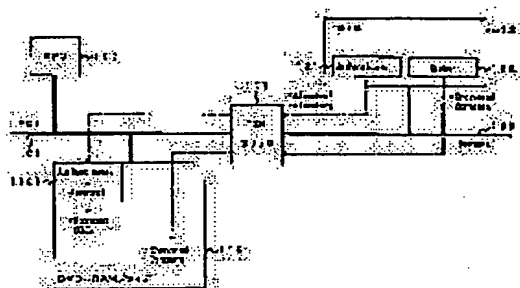
(72)Inventor : ISHIBASHI YASUHIRO
SOGABE HIDEKI

(54) DATA RECORDING DEVICE, DATA PROCESSING SYSTEM USING THE SAME, AND COPY PROTECTING METHOD AND RECORDING MEDIUM

(57)Abstract:

PROBLEM TO BE SOLVED: To realize a storage device capable of safely recording digital contents being objects of copy protection.

SOLUTION: Since an authenticator 1161 for authenticating equipment is provided in the bus interface of a DVD(digital versatile disk)-RAM drive 116, contents which could not be recorded so for whose copy is possible one time can be safely recorded in a storage device by recording transmitted encrypted contents (encrypted contents) as they are. Moreover, only authorized devices are allowed to perform releasing of encryption of storage contents of the storage device by authentication with the storage device by writing content cypher releasing key (K content) in an area which can not be read out from a system.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-306673

(43) 公開日 平成11年(1999)11月5日

(51) Int.Cl.⁶

識別記号

F I

G 1 1 B 20/10

G 1 1 B 20/10

H

H 0 4 L 12/40

G 0 9 C 1/00

6 6 0 D

// G 0 9 C 1/00

6 6 0

H 0 4 L 11/00

3 2 0

審査請求 未請求 請求項の数12 O L (全 17 頁)

(21) 出願番号 特願平10-108118

(22) 出願日 平成10年(1998)4月17日

(71) 出願人 000003078

株式会社東芝

神奈川県川崎市幸区堀川町72番地

(72) 発明者 石橋 泰博

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

(72) 発明者 曾我部 秀樹

東京都青梅市末広町2丁目9番地 株式会
社東芝青梅工場内

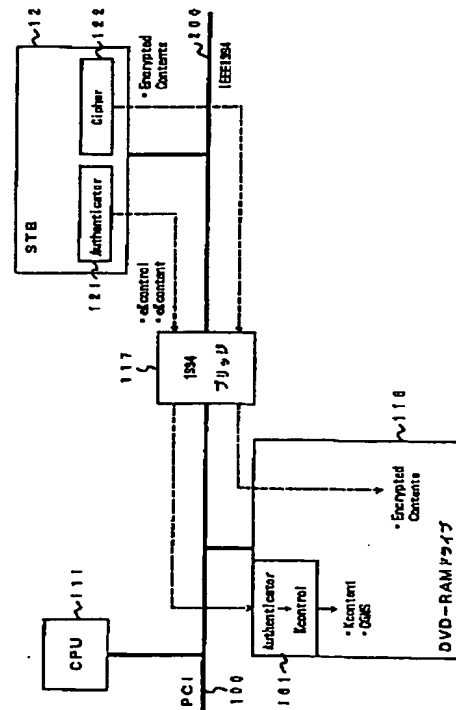
(74) 代理人 弁理士 鈴江 武彦 (外6名)

(54) 【発明の名称】 データ記憶装置、同装置を用いたデータ処理システム、およびコピープロテクト方法並びに記録媒体

(57) 【要約】

【課題】 コピープロテクト対象のデジタルコンテンツを安全に記録することが可能なストレージデバイスを実現する。

【解決手段】 DVD-RAMドライブ116のバスインターフェース部に機器認証用の Authenticator 部1161が設けられており、送られて来た暗号化コンテンツ (Encrypted Contents) を暗号化されたまま記録することにより、今まで、記録できなかった1回コピー可能なコンテンツをストレージデバイスに安全に記録できるようになる。また、コンテンツ暗号解除キー (Kcontent) を、システムから読み出せない領域に書き込むことにより、正当なデバイスだけが、ストレージデバイスとの認証によってそのストレージデバイスの記憶内容の暗号化解除を行うことが可能となる。



【特許請求の範囲】

【請求項 1】 コピープロテクト対象のデータを扱うデータ処理システムで使用されるリード／ライト可能なデータ記憶装置において、

前記コピープロテクト対象のデータを授受する相手先のデバイスとの間で、前記コピープロテクト対象のデータを暗号化して授受するための認証処理を行う認証手段と、

前記相手先のデバイスから暗号化されて送信されるデータを記録媒体上に格納する手段とを具備し、

前記コピープロテクト対象のデータを暗号化したまま記録できるように構成されていることを特徴とするデータ記憶装置。

【請求項 2】 前記認証手段は、前記相手先のデバイスとの間のキー交換処理によって、前記相手先のデバイスから暗号化されて送信される暗号化データを復号化するために必要な暗号化解除キーを生成し、前記暗号化解除キーは、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録されることを特徴とする請求項 1 記載のデータ記憶装置。

【請求項 3】 前記相手先のデバイスから暗号化されて送信される暗号化データは前記記録媒体上のセクタ領域に格納され、前記暗号化解除キーはセクタ間のギャップ領域に格納されることを特徴とする請求項 2 記載のデータ記憶装置。

【請求項 4】 前記相手先のデバイスから暗号化されて送信される暗号化データには、前記暗号化データの種別が一回のみコピー可、これ以上コピー不可、コピー不可、コピーフリーのいずれであるかを示すコピーコントロール情報が含まれており、前記認証手段は、前記コピーコントロール情報が一回のみコピー可を示すとき、そのコピーコントロール情報をこれ以上コピー不可に書き換え、この書き換えられたコピーコントロール情報は、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録されることを特徴とする請求項 1 記載のデータ記憶装置。

【請求項 5】 前記認証手段は、前記記録媒体上に格納された暗号化データを読み出す相手先のデバイスとの間の認証処理によって前記相手先のデバイスが正当なデバイスであることが確認されたとき、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録されている暗号化解除キーを用いて、前記相手先のデバイスに暗号化データを復号化するために必要なキーを生成させるためのキー交換処理を実行することを特徴とする請求項 2 記載のデータ記憶装置。

【請求項 6】 コピープロテクト対象のデータを暗号化して授受するための認証機能を有するデバイスを備えたデータ処理システムにおいて、リード／ライト可能に構成されたデータ記憶装置と、

このデータ記憶装置に設けられ、前記コピープロテクト対象のデータを授受する相手先のデバイスとの間で、前記コピープロテクト対象のデータを暗号化して授受するための認証処理を行う認証手段とを具備し、

前記相手先のデバイスから暗号化されて送信されるデータを前記データ記憶装置の記録媒体上に暗号化したまま記録することを特徴とするデータ処理システム。

【請求項 7】 コピープロテクト対象のデータを扱うデータ処理システムで使用されるリード／ライト可能なデータ記憶装置に適用されるコピープロテクト方法であって、

前記コピープロテクト対象のデータを前記データ記憶装置に書き込むとき、前記コピープロテクト対象のデータの送信側のデバイスと前記データ記憶装置との間で互いのデバイスの正当性を確認するための認証処理を実行し、

この認証処理で互いのデバイスの正当性が確認されたとき、送信側のデバイスにて送信データを暗号化して前記データ記憶装置に送信し、

その暗号化データを前記データ記憶装置の記録媒体上に暗号化したまま記録することを特徴とするコピープロテクト方法。

【請求項 8】 前記データ記憶装置は、前記送信側のデバイスとの間のキー交換処理によって、前記送信側のデバイスから暗号化されて送信される暗号化データを復号化するために必要な暗号化解除キーを生成し、前記暗号化解除キーは、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録されることを特徴とする請求項 7 記載のコピープロテクト方法。

【請求項 9】 前記送信側のデバイスから暗号化されて送信される暗号化データは前記記録媒体上のセクタ領域に格納され、前記暗号化解除キーはセクタ間のギャップ領域に格納されることを特徴とする請求項 8 記載のコピープロテクト方法。

【請求項 10】 前記送信側のデバイスから前記データ記憶装置に暗号化されて送信される暗号化データには、前記暗号化データの種別が一回のみコピー可、これ以上コピー不可、コピー不可、コピーフリーのいずれであるかを示すコピーコントロール情報が含まれており、

前記コピーコントロール情報が一回のみコピー可を示すとき、そのコピーコントロール情報をこれ以上コピー不可に書き換え、

この書き換えられたコピーコントロール情報を、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録することを特徴とする請求項 7 記載のコピープロテクト方法。

【請求項 11】 前記データ記憶装置は、前記記録媒体上に格納された暗号化データを読み出す相手先のデバイスとの間の認証処理によって前記相手先のデバイスが正当なデバイスであることが確認されたとき、前記データ

10

20

30

40

50

処理システムからは読み出せない前記記録媒体上の領域に記録されている暗号化解除キーを用いて、前記相手先のデバイスに暗号化データを復号化するために必要なキーを生成させるためのキー交換処理を実行することを特徴とする請求項7記載のコピープロテクト方法。

【請求項12】 コンピュータシステムによって読み出し可能な記録媒体であって、
コピープロテクト対象のデータが暗号化されて記録される第1記憶領域と、前記暗号化データの暗号化を解除するために必要な暗号化解除キーが記録される第2記憶領域とを含み、前記第2記憶領域は、前記コンピュータシステムからは読み出すことが出来ない領域であることを特徴とする記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】 本発明はデジタルコンテンツを扱うパーソナルコンピュータの補助記憶装置などとして使用されるデータ記憶装置、同記憶装置を用いたデータ処理システム、およびコピープロテクト方法並びに記録媒体に関する。

【0002】

【従来の技術】 近年、コンピュータ技術の発達に伴い、デジタルビデオプレーヤ、セットトップボックス、TV、パーソナルコンピュータ等のマルチメディア対応の電子機器が種々開発されている。

【0003】 この種の電子機器は、例えばDVD (Digital Versatile Disk) に蓄積された映画、デジタル衛星放送によるTV番組等のデジタルコンテンツを再生することができる。

【0004】 デジタルコンテンツは一般にMPEG2という動画像高能率符号化方式を使って符号化された後、記録媒体や、伝送媒体を通じて各家庭に送られる。MPEG2による符号化は、画質と、容量に対する記録時間の双方を確保する観点から、可変レート符号化の考えに基づいている。可変レート符号化データのデータ量は、元の画像の画質に依存し、動きの激しいシーンほどそのデータ量は増加する。よって、デジタルコンテンツは、各家庭にオリジナル映像と遜色のない高画質の映像を提供することができる。

【0005】 近年、このようなデジタルコンテンツの著作権保護等の観点から、その不正コピーを防止するためのコピープロテクト技術の必要性が叫ばれてきたが、有効な手法が構築されていないのが現状である。

【0006】 そこで、CPTWG (Copy Protection Technical Working Group) では、マルチメディアデータの伝送に好適な次世代のバスインターフェイスであるIEEE1394シリアルバスに向けた新たなコピープロテクト方式の仕様(以下、IEEE1394コピープロテクト技術と称する)の策定作業が進められている。

【0007】 IEEE1394シリアルバスは、デジタルビデオプレーヤ、セットトップボックス、TV、パーソナルコンピュータ等をつなぐ次世代のバスインターフェイスであり、転送モードとして、アシンクロナスサブアクションと、アイソクロナスサブアクションの2種類をサポートしている。前者は、非同期転送モードと呼ばれ、リアルタイム性が要求されない一般のデータの転送時に使用される。後者は、転送帯域を保証した同期転送モードであり、ビデオデータやオーディオデータに代表されるデジタルコンテンツのリアルタイム転送が可能である。

【0008】 IEEE1394コピープロテクト技術は、公開鍵暗号化方式や共通鍵暗号化方式などのよく知られた暗号化プロトコルを用いることにより、IEEE1394シリアルバスを介してデジタルビデオプレーヤ、セットトップボックス、TV、パーソナルコンピュータなどの機器間で受け渡しされるデジタルコンテンツを暗号化し、その不正コピーを防止できるようにしている。

20 【0009】

【発明が解決しようとする課題】 しかし、パーソナルコンピュータはもともとオープンなシステムであるため、IEEE1394シリアルバス上に流れるデータを暗号化しただけでは、不正コピーに対する十分な保護を期待することはできない。以下、これについて具体的に説明する。

【0010】 図15は、IEEE1394コピープロテクト技術をそのままパーソナルコンピュータに適用した場合の構成例である。図15においては、パーソナルコンピュータ(PC)1、セットトップボックス(STB)2、およびデジタルビデオカメラ(DVC)3の3つの機器がIEEE1394シリアルバス10を介して接続されている様子が示されている。

【0011】 これらパーソナルコンピュータ(PC)1、セットトップボックス(STB)2、およびデジタルビデオカメラ(DVC)3は、それぞれIEEE1394シリアルバス10とのインターフェイス部に、暗号化部(Cipher)、復号化部(De-Cipher)、または暗号化・復号化双方の機能を持つ暗号化/復号化部(De-/Cipher)を有している。

【0012】 すなわち、IEEE1394シリアルバス10を介して他の機器にデジタルコンテンツの送信を行うデジタルビデオカメラ(DVC)3については暗号化部(Cipher)が設けられ、IEEE1394シリアルバス10を介して他の機器との間でデジタルコンテンツの送受信を行うパーソナルコンピュータ(PC)1およびセットトップボックス(STB)2については暗号化/復号化部(De-/Cipher)が設けられている。

50 【0013】 コピープロテクトが必要なデジタルコンテ

ンツはその送信側の機器によって暗号化された後に I E E E 1 3 9 4 シリアルバス 1 0 上に出力され、その暗号化データは受信側の機器にて復号化されて暗号化が解除される。このように I E E E 1 3 9 4 シリアルバス 1 0 上に流れるデータを暗号化することにより、I E E E 1 3 9 4 シリアルバス 1 0 上に流れるデータが不正にコピーされてもそれが正常に再生されてしまうことを防止することができる。

【0014】パーソナルコンピュータ (PC) 1 においては、暗号化／復号化部 (De-/Cipher) は、
10 図示のように、PCIバス20などのシステムバスと I E E E 1 3 9 4 シリアルバス 1 0 との間を双方向につなぐ 1 3 9 4 ブリッジ 6 内に設けられる。これにより、PCIバス20上には暗号化データは流れず、通常通り平文データだけが流れるので、オープンなバスアーキテクチャを維持できる。

【0015】デジタルビデオカメラ (DVC) 3 またはセットトップボックス (STB) 2 から I E E E 1 3 9 4 シリアルバス 1 0 を介してパーソナルコンピュータ (PC) 1 に伝送される暗号化データは 1 3 9 4 ブリッ
20 ジ 6 によって平文に復号化された後、PCIバス20上の CPU 4 や MPEG デコーダ 5 に送られる。同様に、CPU 4 や MPEG デコーダ 5 からセットトップボックス (STB) 2 にデジタル映像コンテンツを送信するときは、PCIバス20上の平文が 1 3 9 4 ブリッジ 6 によって暗号化された後、I E E E 1 3 9 4 シリアルバス 1 0 上に送り出される。

【0016】このように、1 3 9 4 ブリッジ 6 に暗号化／復号化機能を設けると、PCIバス20のオープンアーキテクチャをそのまま維持することはできるが、PC
30 Iバス20には暗号化が解かれたデータ (Plain Contents) が流れてしまい容易にコピー可能となってしまう。

【0017】このため、PCIバス20上を転送されるデジタルコンテンツについても暗号化できるように新たなシステムを構築することが必要とされている。しかし、一般に、パーソナルコンピュータにおいて補助記憶装置として用いられる DVD-RAM、MO、HDD などの通常のストレージデバイスには認証機能が設けられ
40 てないため、PCIバス20上を転送されるデジタルコンテンツを暗号化すると、コピープロテクトが必要なコンテンツをそれらストレージデバイスに一切記録することが出来なくなってしまう。コピープロテクト対象のデジタルコンテンツには、一回のみコピー可のものや、コピーフリーのものもあるので、このような種類のデジタルコンテンツについてはストレージデバイスに記録できるようにすることが望ましい。

【0018】また、認証機能と復号化機能をストレージデバイスに用意すれば、コンテンツの暗号化を解除した後それをストレージデバイスに記録することが可能と

なるが、このようにすると、今度は、その記録内容 (Plain Contents) が不正に読み出されて使用されるとい危険が生じる。特に、可搬型の記録メディアを使用するリムーバブルストレージデバイスの場合には、コピープロテクト機能を持たないシステムで不正に利用される危険が高い。

【0019】本発明は上述の実情に鑑みてなされたものであり、コピープロテクト対象のデジタルコンテンツを安全に記録することが可能なデータ記録装置、同装置を用いたデータ処理システムおよびおよびコピープロテクト方法並びに記録媒体を提供することを目的とする。

【0020】

【課題を解決するための手段】 上述の課題を解決するため、本発明は、コピープロテクト対象のデータを扱うデータ処理システムで使用されるリード／ライト可能なデータ記憶装置において、前記コピープロテクト対象のデータを授受する相手先のデバイスとの間で、前記コピープロテクト対象のデータを暗号化して授受するための認証処理を行う認証手段と、前記相手先のデバイスから暗号化されて送信されるデータを記録媒体上に格納する手段とを具備し、前記コピープロテクト対象のデータを暗号化したまま記録できるように構成されていることを特徴とする。

【0021】このデータ記憶装置においては、認証手段が設けられており、相手先デバイスとの間の認証処理によって、互いにコピープロテクト対象のデータを扱うことができるデバイスであることが確認されると、相手先デバイスからデジタルコンテンツが暗号化されて送信されて来る。この暗号化データは暗号化されたままデータ記憶装置の記憶媒体上に記録される。このようにデータ記憶装置に認証機能を設けることにより、これまで記録が不可能であった一回のみコピー可などの種類のデジタルコンテンツをデータ記憶装置に記録することが可能となる。また、送られてくる暗号化データをそのまま記憶媒体上に記録しているので、その記録媒体から記憶内容を不正に読み出しても、基のデータに復元することはできない。よって、読み出しは、コピープロテクト機能を持つ正当なデバイスからしか行うことが出来ず、デジタルコンテンツをその不正使用から保護することが可能となる。

【0022】また、データ記憶装置に設けられた認証手段は前記相手先のデバイスとの間のキー交換処理によって、前記相手先のデバイスから暗号化されて送信される暗号化データを復号化するために必要な暗号化解除キーを生成し、この暗号化解除キーは、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録することが好ましい。

【0023】このように暗号化解除キーをシステムからは読み出せない領域に記録しておくことにより、コピープロテクト機能を持つ正当なデバイスに対してのみ暗号

解除キーを渡すことが可能となり、不正なキー読み出しおよびそれをういた暗号化データの復号を防止することができる。

【0024】また、相手先のデバイスから暗号化されて送信される暗号化データは記録媒体上のセクタ領域に格納し、前記暗号化解除キーはセクタ間のギャップ領域に格納することが好ましい。

【0025】また、相手先のデバイスから暗号化されて送信される暗号化データには、前記暗号化データの種別が一回のみコピー可、これ以上コピー不可、コピー不可、コピーフリーのいずれであるかを示すコピーコントロール情報が含まれており、前記認証手段は、前記コピーコントロール情報が一回のみコピー可を示すとき、そのコピーコントロール情報をこれ以上コピー不可に書き換え、この書き換えられたコピーコントロール情報を、前記データ処理システムからは読み出せない前記記録媒体上の領域に記録することが好ましい。

【0026】これにより、一回のみコピー可のデジタルコンテンツについては、一度データ記憶装置に記憶した後は再度記憶することが不可能となり、そのデジタルコンテンツの保護を図ることが可能となる。

【0027】また、このような本発明のデータ記憶装置は、コピープロテクト対象のデータを暗号化して授受するための認証機能を有する外部機器が接続可能な外部バスとのインターフェイスを有するデータ処理システムに適用して用いることが好ましい。すなわち、データ処理システムは、内部バスと、この内部バスにそれぞれ結合され、コピープロテクト対象のデータを前記内部バス経由で送信または受信する複数の機能モジュールと、前記各機能モジュール毎に設けられ、前記コピープロテクト対象のデータを授受する相手先の機能モジュールまたは前記外部機器との間で、前記コピープロテクト対象のデータを暗号化して授受するための認証処理を行う認証手段とを具備し、前記データ処理装置内の各機能モジュール毎に認証処理を行う。これら機能モジュールの一つとして、データ記憶装置を設けることにより、デジタルコンテンツなどのコピープロテクト対象のデータを扱う複数の機能モジュールそれぞれのインターフェイス部に認証手段が設けられることになり、機能モジュール間、あるいは機能モジュールと外部機器間で個別に認証処理を行うことができる。よって、それら機能モジュールが接続された内部バス上には、暗号化解除のためのキー、およびデジタルコンテンツは暗号化されたまま転送されるようになり、デジタルコンテンツの不正コピーを防止することができる。また、機能モジュール毎に認証処理を行っているので、ストレージデバイスや、MPEG2デコーダなど、機能モジュールの種類に応じてそれが扱うことが可能なデジタルコンテンツの種類（一回のみコピー可、コピー不可、コピーフリー）を効率よく制限することが可能となる。

【0028】

【発明の実施の形態】以下、図面を参照して本発明の実施形態を説明する。図1には、本発明の一実施形態に係るパーソナルコンピュータ（以下、PC11と称する）のシステム構成が示されている。このPC11は、IEEE1394シリアルバス200を介して外部のコンシューマ電子機器、たとえば図示のようなセットトップボックス（STB）12、デジタルビデオカメラまたはDVカムコーダ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14と通信可能に構成されている。

【0029】セットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14は、それぞれIEEE1394コピープロテクト技術をサポートするために、IEEE1394シリアルバス200とのインターフェイス部に、デバイス認証およびキー交換などを行う認証処理部（Authenticator）121、131、141を有している。デジタルコンテンツの送受信を行うセットトップボックス（STB）12およびデジタルビデオカセットレコーダ（D-VCR）14については、暗号化・復号化双方の機能を持つ暗号化／復号化部（De-/Cipher）122、142が設けられている。また、デジタルコンテンツの送信のみを行うデジタルビデオカメラ（DVC）13については、暗号化部（Cipher）132だけが設けられている。

【0030】PC11、セットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14間で授受されるデジタルコンテンツは、暗号化された状態でIEEE1394シリアルバス200上を転送される。

【0031】PC11は、図示のように、PCIバス100と、これに接続された複数の機能モジュールとから構成されている。これら機能モジュールの中で、デジタルコンテンツを扱う機能モジュール、つまり、CPUモジュール111、サテライトまたはデジタルTV用のチューナ113、MPEG2デコーダ115、DVD-RAMドライブ116については、PCIバス100とのインターフェイス部に、機器認証およびキー交換などを行う認証処理部（Authenticator）1111、1131、1151、1161が設けられている。これら各認証処理部（Authenticator）1111、1131、1151、1161の機能は、基本的に、1394デバイスであるセットトップボックス（STB）12、デジタルビデオカメラ（DVC）13、およびデジタルビデオカセットレコーダ（D-VCR）14のそれと同じであり、デジタルコンテンツを暗号化して授受するために必要な認証およびキー交換を行

う。

【0032】また、これらCPUモジュール111、チューナ113、MPEG2デコーダ115のインターフェイス部には、さらに、暗号化されたコンテンツ(encrypted contents)の暗号化を解除するための復号化処理を行う復号化部(Decipher)、または暗号化部(Cipher)が設けられている。暗号化部を持つか復号化部を持つか、あるいはその両方を持つかは各機能モジュールの機能によって決まる。ここでは、チューナ113については暗号化部(Cipher)1132が設けられ、CPUモジュール111およびMPEG2デコーダ115については復号化部(Decipher)1112、1152が設けられている場合が例示されている。

【0033】CPUモジュール111は、マイクロプロセッサと、メモリコントローラ、およびPCIバスブリッジなどから構成されており、認証部1111と暗号解除部1112は例えばPCIバスブリッジの一部として組み込むことができる。また、CPUモジュール111内の認証部1111、暗号解除部1112、MPEG2デコーダ部1113はソフトウェアで実現しても良い。

【0034】DVD-RAMドライブ116はPC11の補助記憶装置として設けられたものであり、IDEインターフェイスまたはATAPIインターフェイス等を介してPCIバス100に接続される。DVD-RAMドライブ116は認証処理部1161のみを有し、復号化部(Decipher)、暗号化部(Cipher)については設けられていない。暗号化されたデジタルコンテンツを暗号化した状態のままDVD-RAM116に記録するためである。

【0035】PC11には、さらに、PCIバス100とIEEE1394シリアルバス200間を双方向で接続する1394ブリッジ117が設けられている。1394ブリッジ117には、認証処理部、暗号化部、復号化部はどれも設けられておらず、暗号化されたデジタルコンテンツは暗号化された状態のままPCIバス100からIEEE1394シリアルバス200へ、またIEEE1394シリアルバス200からPCIバス100に転送される。このように、1394ブリッジ117は、PC11内の機能モジュールと1394デバイスとの間を透過的に接続する。

【0036】ここで、IEEE1394シリアルバス200上のDVC13から転送されるデジタルコンテンツを、CPUモジュール111でソフトウェアデコードする場合の処理手順について説明する。

【0037】まず、DVC13とCPUモジュール111との間で機器認証を行い、互いにコピープロテクト機能を有する正当なデバイスであることを確認し合う。この機器認証は、たとえば、ランダムチャレンジ&レスポンス方法や、一方向関数を用いた方法、乱数を用いて毎

回変わる時変キーを使用する方法など、良く知られた方法を用いて実現できる。通信相手のデバイスがどのようなコンテンツの種類を扱うことができるものであるか否かの認証については、システムIDが用いられる。このシステムIDは、1394デバイスおよびPC11内の各機能モジュールの回路またはファームウェアなどに埋め込まれており、これによって、一回のみコピー可、コピー不可、コピーフリーの全種類のデジタルコンテンツを扱えるデバイスであるか、一回のみコピー可あるいはコピーフリーのデジタルコンテンツだけを扱えるデバイスであるかが判別される。

【0038】この認証処理にて、CPUモジュール111はDVC13とキー交換を行い、暗号化されたコンテンツの暗号を解除するためのキーを生成する。認証部がCPUモジュール111内にあるため、キー自身あるいはそれを生成するための情報は暗号化されたまま、1394バス200およびPCIバス100を介してDVC13からCPUモジュール111に転送される。

【0039】DVC13は、デジタルコンテンツを暗号化し、それをCPUモジュール111に送る。暗号化されたコンテンツは暗号化されたまま1394バス200およびPCIバス100を介してCPUモジュール111に届き、CPUモジュール111の復号部(Decipher)1112は認証によって得たキーを使ってコンテンツの暗号を解く。CPUモジュール111の認証部と復号化部がソフトウェアによって実現されている場合には、このソフトウェアを改ざんできない、またはアルゴリズムが分からないような手だてを講じる必要があることはもちろんである。

【0040】暗号を解かれたコンテンツはCPUモジュール111内のソフトウェアMPEG2デコーダ(Decoder)1113によってデコードされた後、主メモリ112とVGAコントローラ114を直接結ぶAGP(Accelerated Graphics Port)を介してVGAコントローラ114に送られて再生される。

【0041】このように、デジタルコンテンツを扱う複数の機能モジュールそれぞれのインターフェイス部に認証処理部と、暗号化あるいは復号化部とを用意し、機能モジュール間あるいは機能モジュールと1394デバイス間でコピープロテクト対象のデジタルコンテンツを受け渡すときに、それらデバイス間で認証処理およびデジタルコンテンツの暗号化・復号化処理を行うことにより、IEEE1394バス200およびPCIバス100のどちらにおいても暗号化解除のためのキー、およびデジタルコンテンツは暗号化されたまま転送されるようになり、デジタルコンテンツの不正コピーを防止することができる。

【0042】また、PC11内の各機能モジュール毎に認証処理を行うことができるので、機能モジュール単位

で扱うことが可能なデジタルコンテンツの種類（一回のみコピー可、コピー不可、コピーフリー）を効率よく制限することが可能となる。

【0043】図2には、図1のシステムにおけるソフトウェアとハードウェアとの関係が示されている。図2において、一点鎖線の上側がソフトウェア、下側がハードウェアである。また、縦方向に階層化されて示されている太枠のブロックがPC11内の各機能モジュールまたは1394デバイスなどのハードウェアデバイスである。

【0044】Authenticatorハンドラは、デジタルコンテンツ再生用ソフトなどのアプリケーションプログラムからの要求に応じて、必要な各ハードウェアデバイスとの間で認証処理やキー交換のための制御を行う。前述したように、1394ブリッジ117はPC11内の各機能モジュールと1394デバイスとを透過的に接続するので、PC11内の各機能モジュールに1394デバイスと同様の認証および暗号化／復号化プロトコルを実装することにより、点線で示されているように、アプリケーションプログラムからはPC11内の各機能モジュールと1394デバイスとを区別することなくそれらを等価に扱うことが可能となる。

【0045】図3には、本実施形態で用いられる認証処理およびキー交換の手順の一例が示されている。コンテンツを送信する側のデバイスがSource Device、受信する側のデバイスがSink Deviceである。

【0046】Sink Deviceは、まず、乱数を使って毎回変わる代わるランダムチャレンジキー(Na)を生成し、認証要求と共にそのランダムチャレンジキー(Na)を、Source Deviceに渡す。そして、Sink Deviceは、決められた関数を用いてNaからArを作成する。

【0047】Source Deviceは、乱数を使って毎回変わる代わるランダムチャレンジキー(Nb)を生成し、それを、認証要求に対する応答としてSink Deviceに返す。そして、Source Deviceは、決められた関数を用いてNbからBrを作成する。

【0048】この後、Source Deviceは、メッセージ(Bv)をSink Deviceに送る。このメッセージ(Bv)は、公開鍵と、Na、Brとから作成されたものである。

【0049】Sink Deviceは、メッセージ(Av)をSource Deviceに送る。メッセージ(Av)は、公開鍵と、Nb、Arとから作成されたものである。

【0050】Source Deviceは、Avが正しいか確認し、正しいければ相手が正当なデバイスであると判断して認証鍵(Ak)を作る。同様に、Sink

Deviceも、Bvが正しいか確認し、正しいければ相手が正当なデバイスであると判断して認証鍵(Ak)を作る。

【0051】この後、Source Deviceは、認証鍵(Ak)で暗号化したコントロール鍵(eKx)をSink Deviceに送る。Sink Deviceは、暗号化されたコントロール鍵(eKx)を認証鍵(Ak)で暗号を解除し、コントロール鍵(Kx)を作る。

10 【0052】なお、図3の認証処理の手順はあくまで一例であり、互いのデバイスが互いに正しいデバイスであることを検証し合うことができるものであれば、前述したように、通常のランダムチャレンジ&レスポンス方法や、その他の良く知られた方法を利用することができる。

20 【0053】次に、転送されるデジタルコンテンツの種類（1回コピー可、コピー不可、コピーフリー）がリアルタイムに切り替わる場合において、扱うことが可能なコンテンツを各デバイス毎に制限する方法について説明する。

【0054】コピー不可、1回のみコピー可のコンテンツを送信可能なデバイスは、コピー不可用と1回のみコピー可用の2種類のコントロールキー（コンテンツ暗号解除キーの暗号化を解くキー）を別々に用意し、受信側のデバイスの能力に応じて、それに渡すコントロールキーの数を変更する。また、受信側のデバイスが両方の（コピー不可、1回のみコピー可）コンテンツを扱える場合は2回認証を行い、両方のコントロールキーを予め取得する。送信側のデバイスにおいて、コンテンツの種類に応じてキーを変更するのは当然のことだが、認証処理によってあらかじめ両方のキーを受信側に準備させておくことにより、コンテンツの種類のダイナミックな切り替えに柔軟に対応することができる。

【0055】以下、この認証処理の具体的な手順の一例を図4のフローチャートを参照して説明する。まず、デジタルコンテンツの送信先となる受信側の各デバイス毎に、以下の処理が行われる。まず、受信側のデバイスからシステムIDを取得する。そして、そのシステムIDに基づいて、その受信側デバイスがコピー不可コンテンツを扱うことができるか否かを判断する（ステップS101）。受信側デバイスがコピー不可コンテンツを扱うことができるデバイスであれば、送信側デバイスから受信側デバイスに対してコピー不可コンテンツ用のコントロールキー(eKcontrol#1)を送信し、受信側デバイスはそのコピー不可コンテンツ用のコントロールキー(eKcontrol#1)を受け取る（ステップS102）。コピー不可コンテンツを扱うことができないデバイスに対しては、コピー不可コンテンツ用のコントロールキーの送信は行われない。

50 【0056】次に、システムIDに基づいて、その受信

側デバイスが1回のみコピー可のコンテンツを扱うことができるかを判断する(ステップS103)。受信側デバイスが1回のみコピー可のコンテンツを扱うことができるデバイスであれば、送信側デバイスから受信側デバイスに対して1回のみコピー可コンテンツ用のコントロールキー(eKcontrol#2)を送信し、受信側デバイスはそのコントロールキー(eKcontrol#2)を受け取る(ステップS104)。1回のみコピー可コンテンツを扱えないデバイスに対しては、1回のみコピー可コンテンツ用のコントロールキーの送信は行われない。

【0057】これら各コントロールキー(eKcontrol#1, #2)は前述したように暗号化されたコンテンツキーの暗号化を解除するためのキーを暗号化したものであり、乱数などを用いた時変キーを用いることができる。受信側のデバイスでは、認証処理で授受される乱数値や予めデバイス内に用意されている他のキーを用いてeKcontrol#1, #2の暗号化を解き、Kcontrol#1, #2が得られる。

【0058】このようにして、各受信側デバイス毎にそのデバイスの機能に応じたキーが渡される。すなわち、コピー不可、1回のみコピー可の両方のコンテンツを扱えるデバイスの場合は2回の認証によって両方のコントロールキーが渡される。また、1回のみコピー可のコンテンツのみを扱えるデバイスの場合には、1回のみコピー可コンテンツ用のコントロールキーのみが渡されることになる。

【0059】全ての受信側デバイスとの認証処理が終了すると(ステップS105)、暗号化されたコンテンツキー(eKcontent)と、暗号化されたコンテンツ(Encrypted contents)とが、送信側デバイスから全ての受信側デバイスにブロードキャスト送信される(ステップS106, S107)。暗号化されたコンテンツ(Encrypted contents)のヘッダ部には、コピー不可、1回のみコピー可、コピーフリーのいずれかを示すコピーコントロール情報(CGMS)が埋め込まれている。

【0060】受信側の各デバイスは、コピーコントロール情報(CGMS)を、コントロールキーを動的に変更するためのコンテンツ識別情報として使用する。すなわち、受信側の各デバイスは、暗号化されたコンテンツに含まれるコピーコントロール情報(CGMS)に従って現在受信処理中のコンテンツの種類を判別し、そのコンテンツの種類に対応したコントロールキー(Kcontrol)を選択する。そして、その選択したコントロールキーを用いることによって、暗号化されたコンテンツキー(eKcontent)の暗号化を解除し、暗号化されたコンテンツ(Encrypted contents)の暗号化を解除するためのコンテンツキー(Kcontent)を生成する(ステップS108)。扱え

ない種類のコンテンツを受信した受信側のデバイスについては、対応するコントロールキー(Kcontrol)が無いのでそのコンテンツの暗号化を解除することは出来ない。

【0061】このように、本実施形態では、種類の異なる複数種のコンテンツから構成されるストリームを送信するときは、受信側のデバイスが扱うことができるコンテンツの種類数だけ認証処理を行い、ストリームを構成するコンテンツの種類の中で受信側のデバイスが処理可能なコンテンツの種類数に対応する暗号化解除用のキーをその受信側のデバイスに渡すという処理が行われる。

【0062】ここで、例えば図5のように、一回のみコピー可のコンテンツからなる暗号化サブストリームAとコピー不可のコンテンツからなる暗号化サブストリームBとを連続して送信する場合を想定する。

【0063】各暗号化サブストリームA, Bの各々のヘッダ部には、図6に示すように、使用するキーの変更を指示するための情報として、コンテンツの種類を示すコンテンツ識別情報が埋め込まれている。このコンテンツ識別情報としては、前述したようにコピーコントロール情報(CGMS)を使用することができる。

【0064】このような暗号化ストリームを、コピー不可、1回のみコピー可の両方のコンテンツを扱えるデバイス(デバイス#1)と、1回のみコピー可のコンテンツもしくはコピーフリーのコンテンツのみを扱えるデバイス(デバイス#2)に送信する場合には、デバイス#1については暗号化サブストリームA, B双方の暗号化解除キーが渡され、デバイス#2については暗号化サブストリームBの暗号化解除キーだけが渡されることになる。

【0065】したがって、図7(a)に示されているように、デバイス#1は、暗号化サブストリームAから暗号化サブストリームBにコンテンツの種類が切り替わった時に、それに応じて暗号化解除キーを動的に変更することにより、暗号化サブストリームA, Bそれぞれに対応する正しい復号データ(平文)を得ることができる。一方、図7(b)に示されているように、デバイス#2は、暗号化サブストリームBの暗号化を解除するためのキーを有していないので、暗号化サブストリームAに対応する復号データ(平文)を得ることは出来るが、暗号化サブストリームBについてはその暗号化を解除することはできない。

【0066】なお、ここでは、各受信側デバイス毎にそのデバイスの機能に応じたコントロールキーを渡すようにしたが、各受信側デバイス毎にそのデバイスの機能に応じたコンテンツキーを準備させることが肝要であるので、そのための手順としては使用する認証処理の方法により様々な手法を用いることができる。また、各機能モジュール毎に認証部や暗号化/復号化部を設ける構成は、PCのみならず、例えば、デジタルコンテンツの録

画／再生用プレーヤなどの各種マイクロコンピュータ応用装置に適用することができる。

【0067】次に、図8を参照して、図1のPC11においてコンテンツをストレージデバイスに記録する方法について説明する。一般に、パーソナルコンピュータにおいて補助記憶装置として用いられるストレージデバイスには認証機能が設けられてないため、コピープロテクトが必要なコンテンツを記録することはできない。また、認証機能と復号化機能を用意すればコンテンツの暗号化を解除した後にストレージデバイスに記録することが可能となるが、このようにすると、今度は、その記録内容(Plain Contents)が不正に使用されてしまう危険がある。特に、可搬型の記録メディアを使用するリムーバブルストレージデバイスの場合には、その危険が高い。

【0068】そこで、本実施形態では、ストレージデバイスには認証処理部(Authenticator)のみを設け、コンテンツを暗号化したまま記録メディアに記録すると共に、さらに認証によって生成されたコンテンツキーを、システムがアクセスできない記録メディア上の領域に記録するようにしている。

【0069】以下、コピープロテクトが必要な一回のみコピー可のデジタルコンテンツをSTB12から受信してDVD-RAMドライブ116のDVD-RAMメディアに記録する場合を例示してその記録方法について具体的に説明する。

【0070】1. STB12とDVD-RAMドライブ116それぞれの認証部(Authenticator)121, 1161を使って、それらデバイス間の認証を行い、互いに正当なデバイスであることが確認されると、STB12側から暗号化されて送られて来るコントロールキー(eKcontrol)をDVD-RAMドライブ116側で暗号を解きコントロールキー(Kcontrol)を生成する。

【0071】2. STB12から暗号化されたコンテンツキー(ekcontent)が暗号化されたデジタルコンテンツと共にDVD-RAMドライブ116に送られる。

【0072】3. 暗号化されたデジタルコンテンツにはコピーコントロール情報(CGMS)が含まれている。4. DVD-RAMドライブ116はKcontrolとCGMSを使ってeKcontentからコンテンツキー(Kcontent)を生成する。eKcontentは時変キーである。

【0073】5. Kcontentで暗号化された暗号化コンテンツ(Encrypted Contents)はそのままメディアの上に記録され、対応するKcontentは例えば図9のようにセクター間のギャップ領域に記録される。またCGMSの内容は“1回コピー可能”から“これ以上コピー不可”の状態に変更さ

れ、同様にこのギャップ領域に記録する。このギャップ領域はシステムからはアクセスできない領域である。

【0074】なお、これら手順のコントロールはすべてCPUモジュール111によって行われる。次に、図10を参照して、DVD-RAMメディアに記録された暗号化コンテンツ(Encrypted Contents)を再生する場合について説明する。

【0075】1. DVD-RAMドライブ116とMP EG2デコーダ115との間で、認証を行う。

2. 互いに正当なデバイスであることが確認されると、暗号化されたコントロールキー(eKcontrol)がDVD-RAMドライブ116からMPEG2デコーダ115に送られる。

【0076】3. MPEG2デコーダ115内のAuthenticator1151でeKcontrolの暗号化を解き、Kcontrolが作られる。

4. 暗号化コンテンツ(Encrypted Contents)と同時に暗号化されたコンテンツキー(ekcontent)とCGMSがDVD-RAMドライブ116からMPEG2デコーダ115へ送られる。

【0077】5. MPEG2デコーダ115のAuthenticator1151でKcontrolとCGMSからekcontentの暗号化を解きKcontentを生成する。

【0078】6. MPEG2デコーダ115内のDe-Cipher1152にKcontentを送る。

7. De-Cipher1152はコンテンツキーにより暗号化コンテンツ(Encrypted Contents)の暗号化を解き、そのコンテンツのPlain Textを生成する。

【0079】8. MPEG2デコーダ115はPlain Textをデコードした後にVGAコントローラ114のビデオ入力ポートに送り、それを画面表示する。

以上のように、ストレージデバイスのバスインターフェース部に機器認証用のAuthenticator部を設け、送られて来た暗号化コンテンツをそのまま記録することにより、今まで、記録できなかった1回コピー可能なコンテンツをストレージデバイスに記録できるようになる。また、送られて来たコンテンツをそのまま記録することにより、コンテンツ暗号解除のための復号化回路が不要になる。また、暗号化解除されたコンテンツ暗号解除キーを、システムから読み出せない領域に書き込むことにより、正当なデバイスだけが、ストレージデバイスとの認証によってそのストレージデバイスの記憶内容の暗号化解除を行うことが可能となる。

【0080】また、このように暗号化されたデジタルコンテンツが通常の領域に記録され、その暗号化解除のためのキーがシステムからは読み出しできない領域に記録されるコンピュータ読み取り可能な記録媒体を用いて各種タイトルを配布するようにしてもよい。これにより、

認証および暗号化／復号化機能を持つ正当な機器でしかその記録媒体の内容を再生できなくなり、不正コピーを防止することが可能となる。

【0081】なお、ここでは、ストレージデバイスとしてDVD-RAMドライブを例示したが、DVD-Rドライブ、MOドライブ、HDDなどに適用しても良い。また、このように認証機能を有するストレージデバイスはPCのみならず、例えばDVDプレーヤとD-VCRの複合機など、リード／ライト可能なストレージデバイスを使用する各種マイクロコンピュータ応用装置に適用10
することができる。また、IEEE1394デバイスとして実現してもよいことはもちろんである。

【0082】次に、暗号化して転送されるコンテンツの属性（分野、地域）を用いて、そのコンテンツを扱うことができるデバイスを制限するというデータ転送制限方法について説明する。

【0083】すなわち、これまでは、コピー不可、一回のみコピー化、コピーフリーというコピー制御情報に基づいてそれを扱うことができるデバイスを制限する方法20
について説明したが、この方法は、基本的には、同一種類のコンテンツからなるストリーム全体を単位とした制御である。したがって、扱うことが許された種類のコンテンツの中で、ある特定の条件に適合した部分だけを扱えるようにするといったきめ細かな制御を行うことは困難である。

【0084】そこで、本データ転送制限方法では、ストリームデータのヘッダ部にコンテンツの内容を示す分野情報や地域情報を埋め込み、それら分野情報や地域情報を用いることにより、扱うことが許された種類（コピー不可、一回のみコピー化、またはコピーフリー）のコン20
テンツからなるストリームの中で、ユーザ等によって予め指定された条件（分野、地域）に適合する部分のみを処理可能にし、それ以外の他の部分については処理できないようにしている。

【0085】図11には、本データ転送制限方法を実現するためのシステム構成が示されている。まず、ストリームデータの packets ヘッダ部に付加された分野情報に応じた転送制御について説明する。

【0086】ここでいう、「分野」とは性的描写の有無・程度、暴力的描写の有無・程度、などの社会的、教育的に要請される分類を意味する。ストリームデータはネットワーク経路の通過時点で packets 化され、この packets はデータの情報を持つヘッダ部とデータそのものから構成される。なお、ここでいうヘッダ部とはネットワーク経路が規定するヘッダであっても、データが内包するヘッダ部分であってもかまわない。

【0087】データ出力システム301はストリームデータの記憶装置302とそれを外部に出力するインタフェース部303とから構成される。ここで、ネットワーク経路に出力すべきデータ packets を作成する。「分30
野」の情報は、図12のようにその packets のヘッダ部に格納される。ネットワークは有線・無線の別を問わない。また、図1のIEEE1394シリアルバス200やPCIバス100などであってもよい。

野」の情報は、図12のようにその packets のヘッダ部に格納される。ネットワークは有線・無線の別を問わない。また、図1のIEEE1394シリアルバス200やPCIバス100などであってもよい。

【0088】データ処理システム401はストリームデータを受け取る装置内にある。例えば、図1のPC11においては、チューナ113、CPUモジュール111、あるいはMPEG2デコーダ115などがデータ処理システム401に相当することになる。また、データ処理システム401はPCのみならず、図の1394デバイスであってよく、またサテライト端末やインターネット端末であってもよい。

【0089】データ処理システム401は実際にデータをユーザに提示するための処理を行う部分で、データを受け取るインタフェース部402と処理を行うストリームデータ処理部403とから構成される。すなわち、「分野」情報はデータを受信した時点ではなくデータ自身を処理するタイミングで解読され、データ処理システム401のユーザ等によって予め設定されたシステム属性情報で定義される分野、との比較によってそのデータの処理の可否がデータ packets 単位で決定される。

【0090】なお、インタフェース部はソフトウェアのみ、ハードウェアのみ、両者の結合体のいずれでもよい。また、ストリームデータには「分野」情報のみならず、その代わりに、あるいはそれに追加して、対応するコンテンツを処理可能な地域を特定するための「地域」情報を埋め込むようにしても良い。ここで、「地域」とはストリームデータの作成者、または配信者の意図に応じて分類されたものである。この場合にも、「地域」情報はデータを受信した時点ではなくデータ自身を処理するタイミングで解読され、データ処理システム401のシステム情報で規定された地域との比較によってそのデータの処理の可否がデータ packets 単位で決定される。

【0091】図13には、ストリームの packets ヘッダに埋め込まれた「分野」、「地域」などのストリーム属性情報によってデータの処理の可否を制御する様子が示されている。

【0092】図13においては、データ処理システム401が扱うことが可能な種類のデジタルコンテンツがデータ packets A, B, C, Dから構成されており、各データ packets 毎にそのヘッダ部に「分野」または「地域」情報がストリーム属性情報として含まれている場合が示されている。

【0093】データ処理システム401のストリーム制限機能により、データ処理システム401に適合する「分野」または「地域」のデータ（データA、データC）だけが処理され、他のデータ（データB、データD）は処理対象から除外され廃棄される。ストリーム制限機能の処理は、図14のフローチャートに示す手順によって実行される。すなわち、まず、データ処理システ30
50

ム 401 に設定されているシステム属性情報が取得され、受信したストリームのパケットヘッダに含まれているストリーム属性情報との比較が行われる（ステップ S201～S204）。一致しているならば、そのストリーム（パケット）の処理が行われ（ステップ S205）、不一致ならば処理されない（ステップ S206）。

【0094】したがって、例えば、図 1 の MPEG2 デコーダ 115 にデータ処理システム 401 のストリーム制限機能を付加した場合には、連続して転送される映像コンテンツ（データ A、B、C、D）の中で、ユーザ設定の「分野」または「地域」に合致するデータ（データ A、データ C）だけがデコードおよび再生され、他のデータ（データ B、データ D）についてはそのデコードおよび再生が行われない。つまり、データ A が再生された後、データ B の再生期間はブランキングとなり、データ B の再生期間が終わるとデータ C が再生されることになる。

【0095】よって、図 11 のシステム構成をサテライト TV 放送などのように不特定多数を相手とするコンテンツ提供システムに適用することにより、各ユーザの条件に合致したシーンだけを再生したり、記録することが可能となり、扱うことが許された種類のコンテンツの中で、ある特定の条件に適合した部分だけを扱えるようにするといったきめ細かな制御を容易に実現できるようになる。

【0096】

【発明の効果】以上説明したように、本発明によれば、ストレージデバイスのバスインターフェース部に機器認証用の Authenticator 部を設け、送られて来た暗号化コンテンツをそのまま記録することにより、今まで、記録できなかった 1 回コピー可能なコンテンツをストレージデバイスに記録できるようになる。また、送られて来たコンテンツをそのまま記録することにより、コンテンツ暗号解除のための復号化回路が不要になる。また、暗号化解除されたコンテンツ暗号解除キーを、システムから読み出せない領域に書き込むことにより、正当なデバイスだけが、ストレージデバイスとの認証によってそのストレージデバイスの記憶内容の暗号化解除を行うことが可能となる。また、暗号化されたデジタルコンテンツが通常の領域に記録され、その暗号化解除のためのキーがシステムからは読み出しできない領域に記録されるコンピュータ読み取り可能な記録媒体を用いて各種タイトルを配布するようにしてもよい。これにより、認証および暗号化／復号化機能を持つ正当な機器でしかその記録媒体の内容を再生できなくなり、不正コピーを防止することが可能となる。

【図面の簡単な説明】

【図 1】本発明の一実施形態に係るコンピュータシステムのシステム構成を示すブロック図。

【図 2】図 1 のシステムにおけるソフトウェアとハードウェアとの関係を示す図。

【図 3】図 1 のシステムにおける機器認証およびキー交換の一例を示す図。

【図 4】同実施形態のシステムで使用される認証処理の具体的な手順の一例を示すフローチャート。

【図 5】同実施形態のシステムに適用されるデジタルコンテンツのストリーム構成の一例を示す図。

【図 6】同実施形態のシステムに適用されるデジタルコンテンツのパケットヘッダにコンテンツ識別情報を付加した様子を示す図。

【図 7】同実施形態のシステムに適用されるデジタルコンテンツ制限処理の原理を説明するための図。

【図 8】同実施形態のシステムに設けられたストレージデバイスへのコンテンツ記録動作を説明するための図。

【図 9】同実施形態のシステムに設けられたストレージデバイスにおけるキーの記憶方式を説明するための図。

【図 10】同実施形態のシステムに設けられたストレージデバイスに記録されているコンテンツの再生動作を説明するための図。

【図 11】同実施形態のシステムに適用されるデータ転送制限方法の原理を説明するための図。

【図 12】図 11 のデータ転送制限方法で使用されるストリームデータの構造の一例を示す図。

【図 13】図 11 のデータ転送制限方法によるデータ制限処理動作を示す図。

【図 14】図 11 のデータ転送制限方法の処理手順を示すフローチャート。

【図 15】1394ブリッジに暗号化／復号化機能を設けたコンピュータシステムのシステム構成を示すブロック図。

【符号の説明】

- 11…パーソナルコンピュータ（PC）
- 12…セットトップボックス（STB）
- 13…デジタルビデオカメラまたはDVカムコーダ（DVC）
- 14…デジタルビデオカセットレコーダ（D-VCR）
- 111…CPUモジュール
- 112…主メモリ
- 113…サイライトまたはデジタルTVチューナ
- 114…VGAコントローラ
- 115…MPEG2デコーダ
- 116…DVD-RAMドライブ
- 117…1394ブリッジ
- 121…認証部（Authenticator）
- 122…暗号化・復号化部（De-/Cipher）
- 131…認証部（Authenticator）
- 132…暗号化部（Cipher）
- 141…認証部（Authenticator）
- 142…暗号化・復号化部（De-/Cipher）

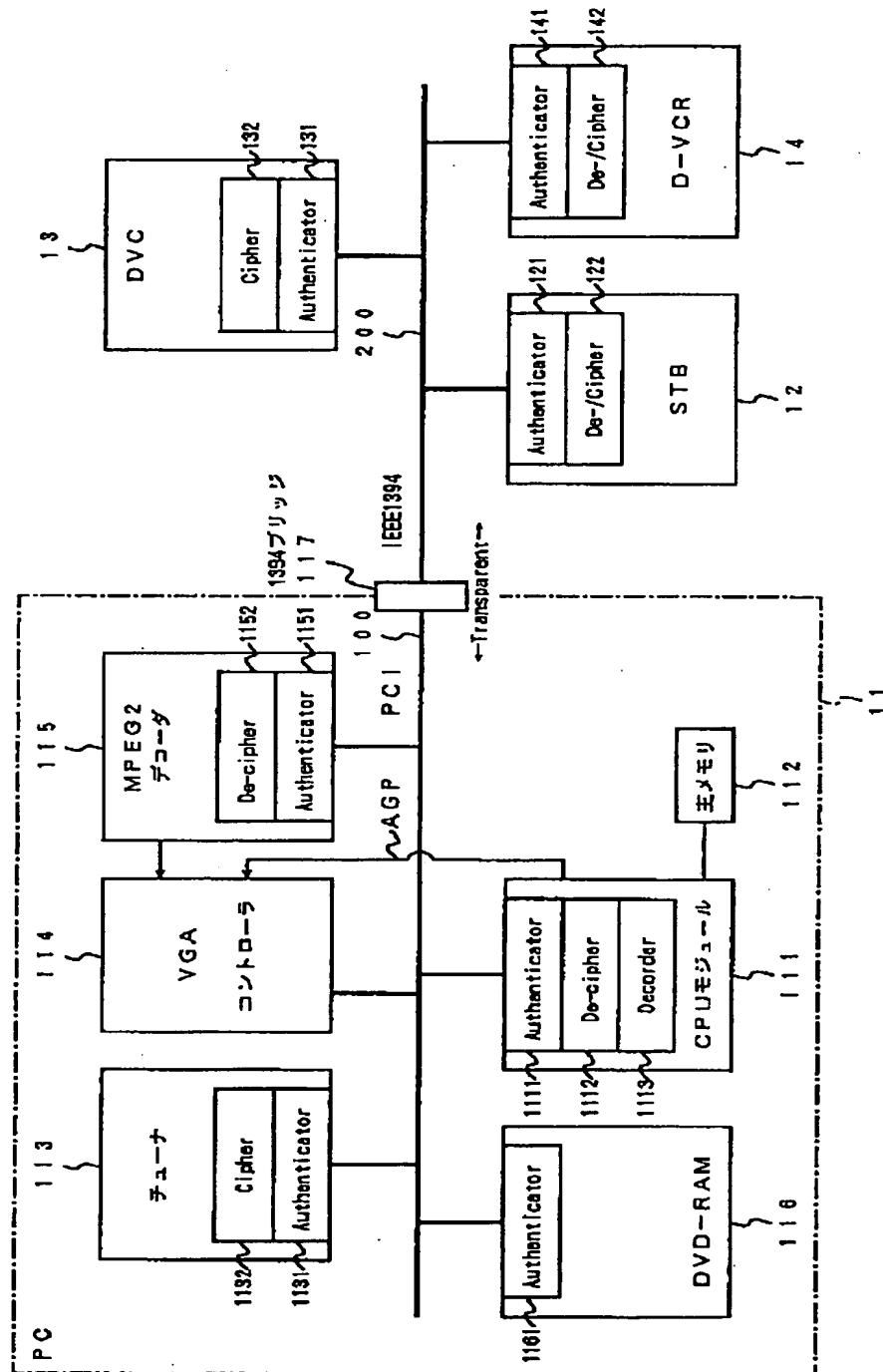
21

22

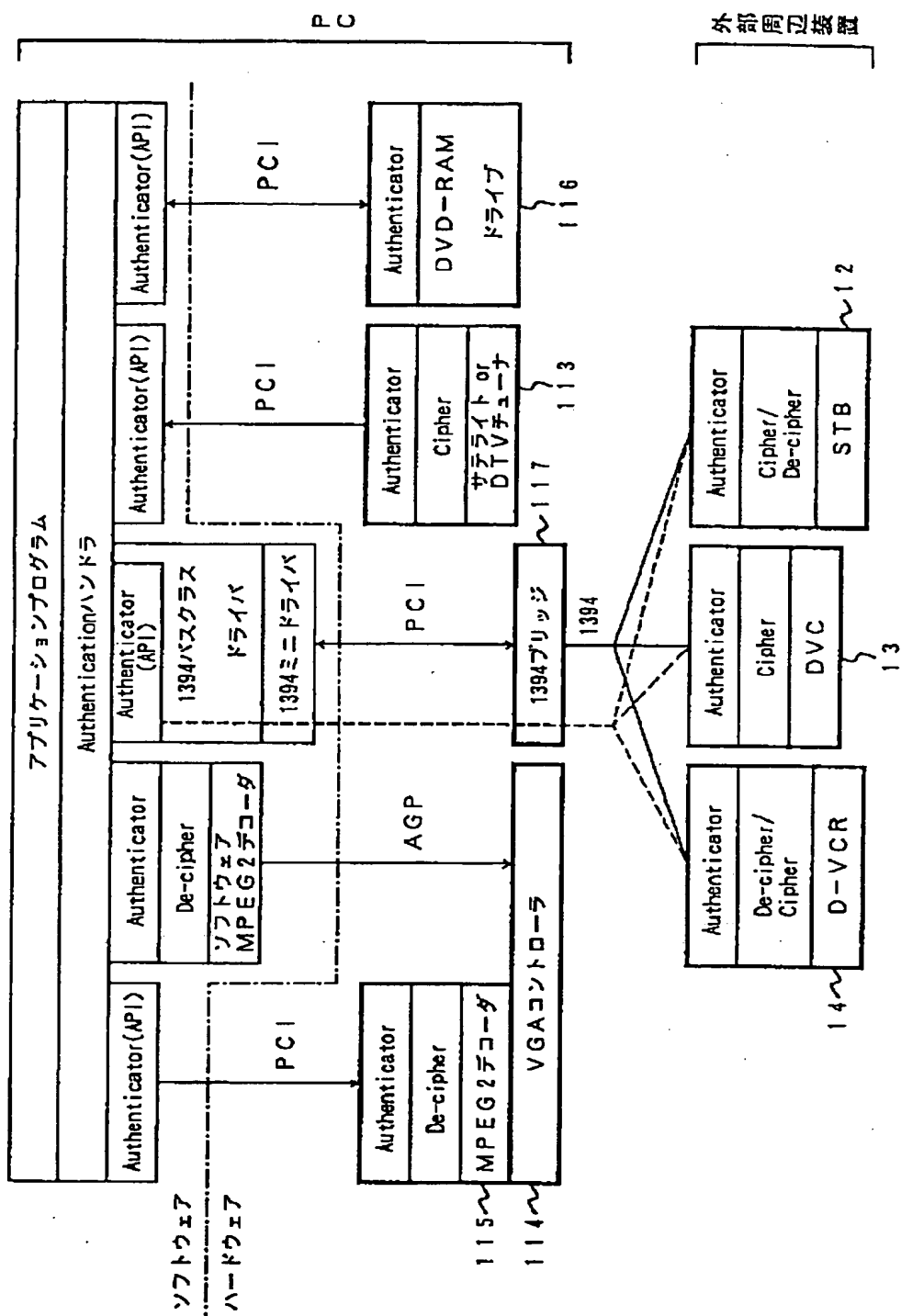
1111…認証部 (Authenticator)
 1112…復号化部 (De-cipher)
 1131…認証部 (Authenticator)
 1132…暗号化部 (Cipher)

1151…認証部 (Authenticator)
 1152…復号化部 (De-cipher)
 1161…認証部 (Authenticator)

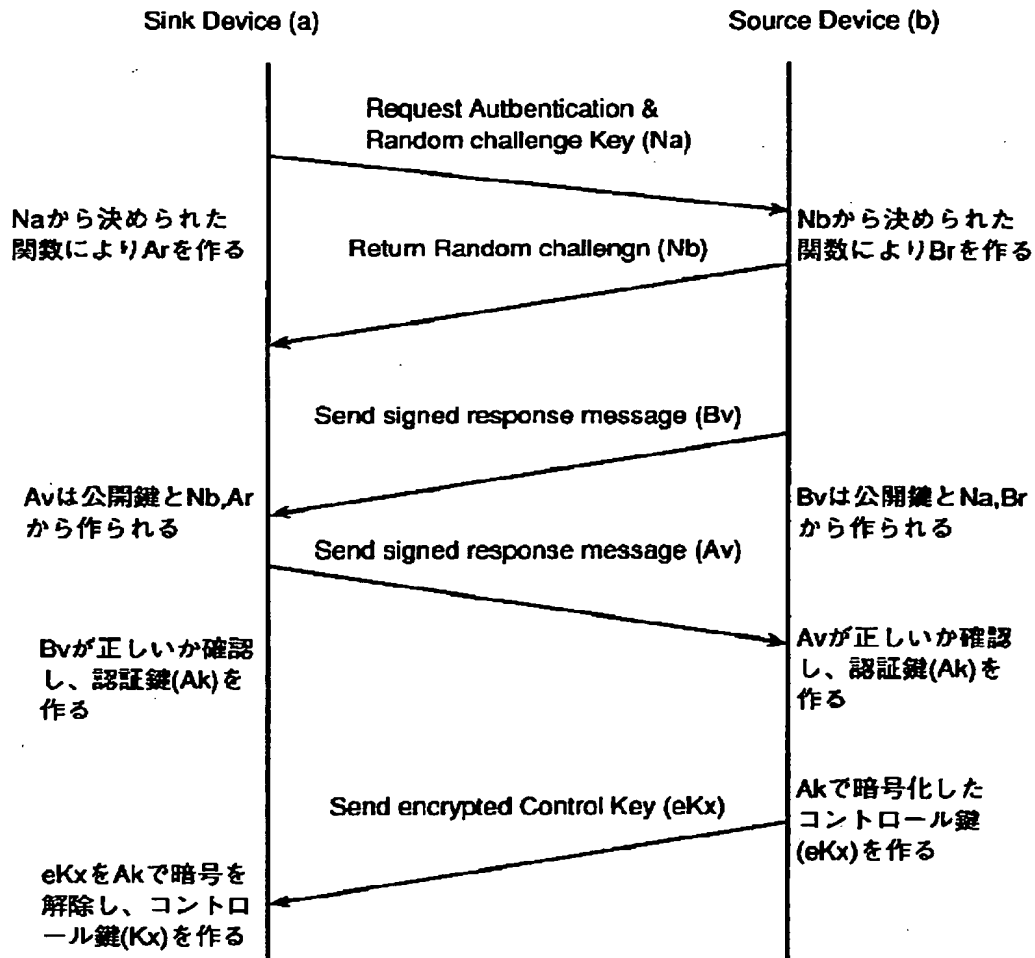
【図1】



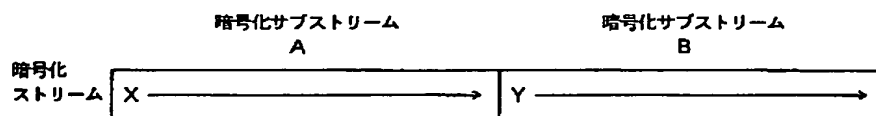
【図2】



【図 3】



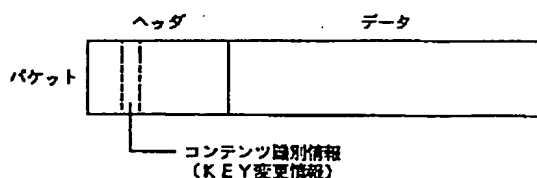
【図 5】



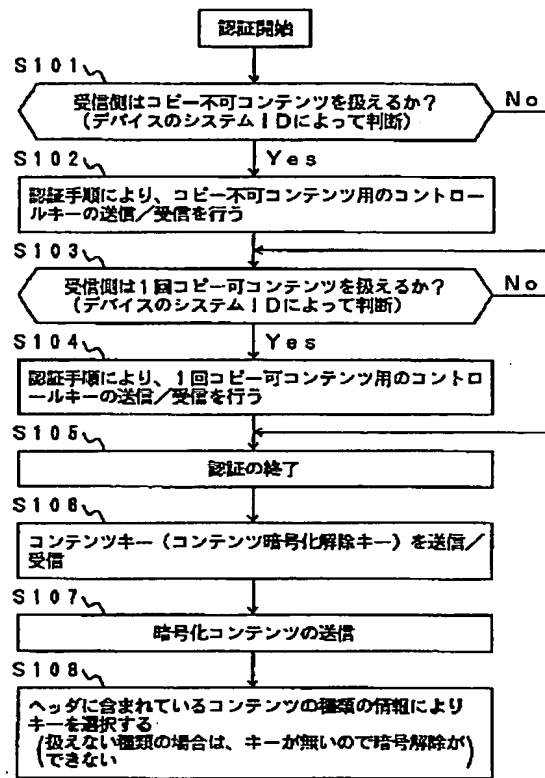
サブストリームA: 1回のみコピー可/暗号鍵X

サブストリームB: コピー不可/暗号鍵Y

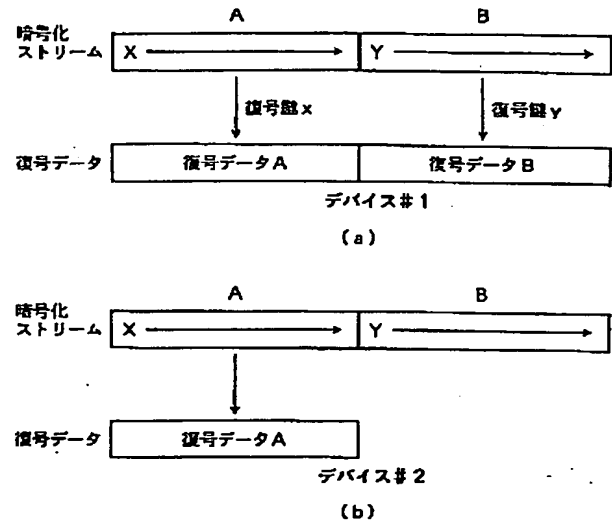
【図 6】



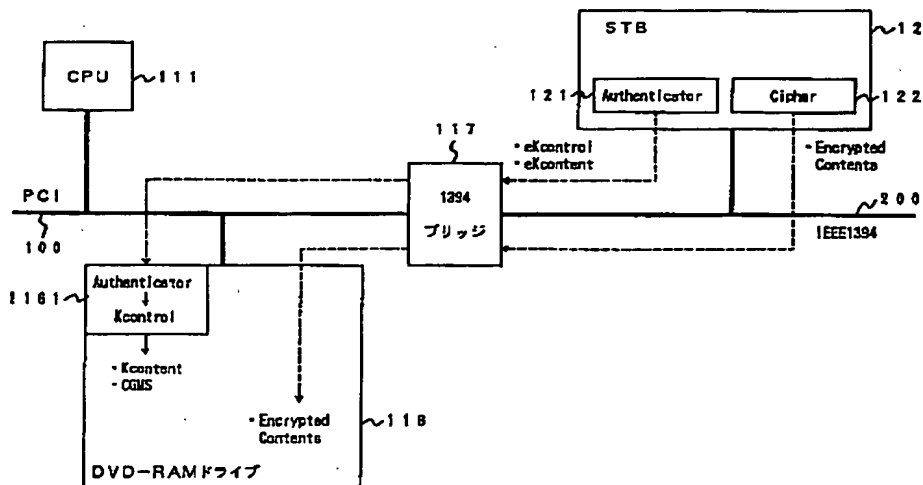
【図4】



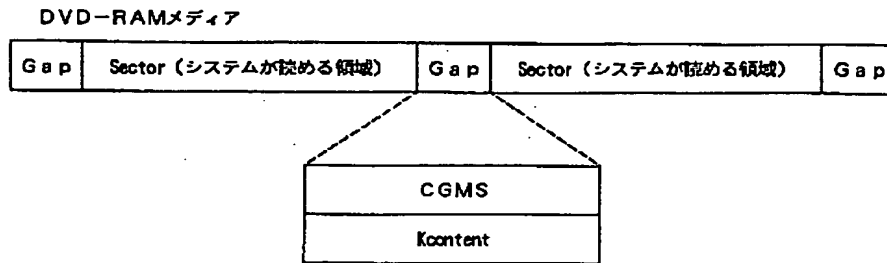
【図7】



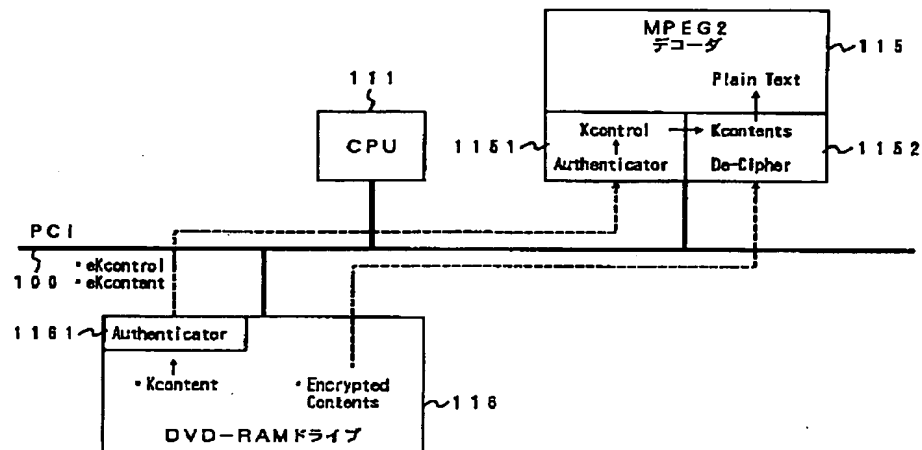
【図8】



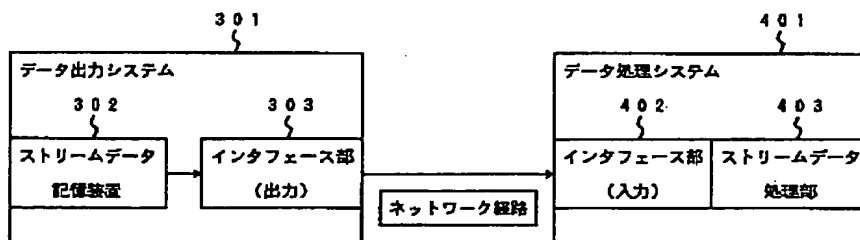
【図9】



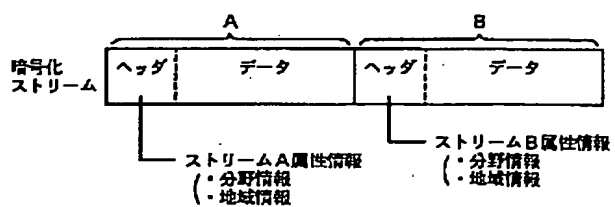
【図10】



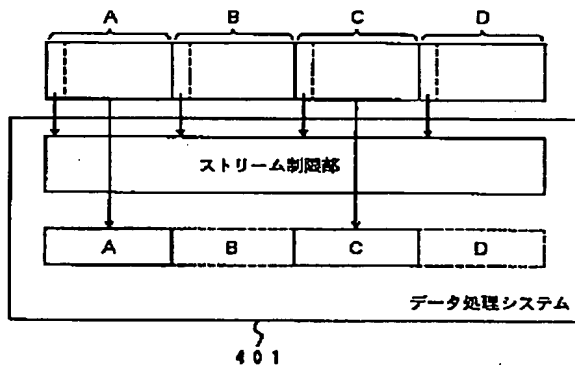
【図11】



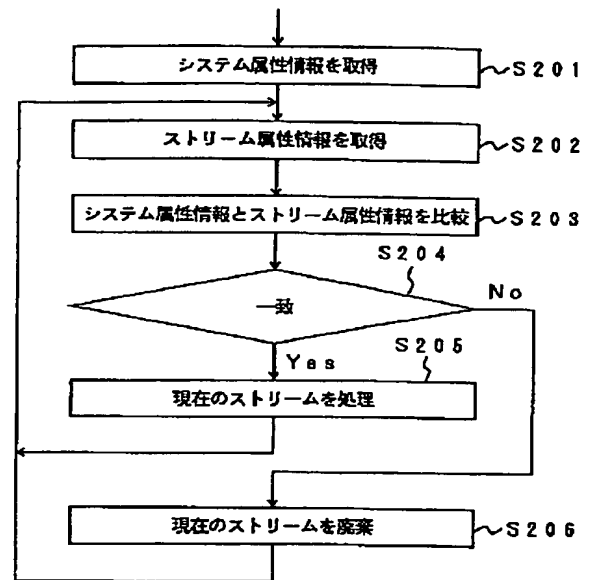
【図12】



【図13】



【図14】



【図15】

